Presidency of the Council of Ministers

THE NATIONAL PLAN FOR CYBERSPACE PROTECTION AND ICT SECURITY

December 2013

Presidency of the Council of Ministers

THE NATIONAL PLAN FOR CYBERSPACE PROTECTION AND ICT SECURITY

December 2013

INDEX

PREFACE

The present National Plan identifies the operational guidelines, the goals to pursue and the lines of action to be carried out in order to give full implementation to the National Strategic Framework for Cyberspace Security, in line with what is outlined by the Prime Minister's Decree of 24th January 2013 setting out "Strategic Guidelines for the National Cyberspace Protection and ICT security".

With this additional document, Italy adopts an integrated strategy which requires the active involvement both of the private and public stakeholders identified in the National Strategic Framework as well as of all those who, on a daily basis, make use of modern ICT technologies, starting with each and every citizen.

Such strategy is structured and yet flexible, as required by the fast technological changes that take place in cyberspace and that are at the origin of innovative security challenges. We need to be not only "up to date", but also forward-looking, so as to prevent future threats aimed at undermining our economic, social, scientific and industrial development, as well as the political and military stability of our country.

INTRODUCTION

The present National Plan (NP) for the cyberspace protection and ICT security aims to implement, for the years 2014-2015, the six strategic guidelines identified in the National Strategic Framework (NSF). In order to give full operability to these strategic guidelines, the National Plan details the eleven operational guidelines identified in the National Strategic Framework, establishing specific objectives and consequent lines of action, as specified in art. 3 first subsection letter b) of the Prime Minister's Decree of 24th January 2013 containing the "guidelines for national cybernetic protection and IT security".

NATIONAL STRATEGIC FRAMEWORK

Strategic Guidelines

1. Enhancement of the technical, operational and analytic capabilities of all concerned stakeholders and institutions through a joint effort and a coordinated approach
2. Strengthening of our capabilities to protect national critical infrastructures and strategic assets and stakeholders
3. Facilitation of all public-private partnerships
4. Promotion and dissemination of the Culture of Cybersecurity
5. Reinforcement of our capability to effectively contrast online criminal activities and illegal contents
6. Strengthening of international cooperation

The National Plan sets out the roadmap for the adoption of the priority measures for implementing the National Strategic Framework by the public and private subjects identified in the Prime Minister's Decree. Since national cyberspace protection and ICT security are not only a goal, but, most importantly, a process, the roadmap for the adoption of priority measures for the implementation of the National Strategic Framework will be pursued through an active and continual dialogue among all actors involved, at various degree, with cybersecurity issues.

The relation between the NSF and the NP is illustrated in the following figure.

NATIONAL PLAN

Operational Guidelines

1. Strengthening of intelligence, police, civil protection and military defense capabilities
2. Enhancement of the organization, coordination and dialogue between national private and public stakeholders
3. Promotion and dissemination of the Culture of Cybersecurity. Education and training
4. International cooperation and exercises
5. Implementation of national CERT, CERT-PA and ministerial CERTs
6. Promotion of *ad hoc* legislation and compliance with international obligations
7. Compliance with standard security requirements and protocols
8. Support to industrial and technological development
9. Strategic communication
10. Resources
11. Implementation of a national system of Information Risk Management

The terminology used in the present National Plan is coherent with the one adopted at the international level (UN, NATO, EU) and with the "Intelligence Glossary" published by the Department for Intelligence and Security (DIS).

The National Plan is the result of the work carried out by the Cybersecurity Working Group (CWG) – established on the 3rd of April 2013 within the Committee for the Security of the Republic at Working Level (the so called "Technical CISR") – chaired by the Department for Intelligence and Security (DIS) - following the adoption of the Prime Minister's "Decree containing Strategic Guidelines for the National Cyberspace Protection and ICT Security" of the 24th January 2013. The work of the CWG is the result of the joint efforts of all points of contact for cybersecurity matters in the Administrations already represented in the Committee for the Security of the Republic (Ministries of Foreign Affairs, Interior, Defence, Justice, Economy and Finance, Economic Development), and included the Agency in charge for the Italian Digital Agenda as well as the Cybersecurity Unit within the Prime Minister Military Advisor's Office.

This inclusive approach will have to be extended so as to engage many other institutional stakeholders such as the Minister of Infrastructures and Transports, the Minister for Education, University and Research, as well as other national public entities.

Furthermore, the National Plan has to be shared with private stakeholders that are essential actors to develop public-private partnerships, and are indispensable for the development of an efficient cybersecurity national defense capability.

The implementation of the operational guidelines highlighted in the present document, which will be developed incrementally, will be measured against a *ad hoc* matrix elaborated by the CWG in order for the CISR at Working Level to be able to carry out the necessary actions for "verifying the implementation of the engagements foreseen in the NP for the security of cyberspace and for the effectiveness of the coordinating procedures among the various private and public stakeholder", in accordance with art 5 subsection 3 letter c) of Prime Minister's Decree of 24th January 2013.

OPERATIONAL GUIDELINE 1

STRENGTHENING OF INTELLIGENCE, POLICE, CIVIL AND MILITARY DEFENSE CAPABILITIES

In order to make ICT networks and computer systems more resilient, especially those supporting critical infrastructures, and to assure, at the same time, a successful contrast of illegal activities, an effective cyber protection and ICT security, it will be required, first of all, a deep understanding of the vulnerabilities – not only technological but also due to human factors – as well as of the cyber threats that may exploit these vulnerabilities.

1.1 ***Assessment of the threats and vulnerabilities***	a. Assess and evaluate cyber threats and vulnerabilities on a regular basis b. Monitor technological innovations in all sectors relying on the use of ICT systems and platforms (industrial processes, critical infrastructures, telemedicine technology, automotive, social networks, data centers, cloud computing, etc.) in order to highlight early-on any possible vulnerability c. Share cybersecurity assessments with all those responsible for critical infrastructures by means of apposite institutional platforms d. Cooperate with universities and public and private research centers to elaborate innovative methodologies and technologies for the detection and the analysis of threats and vulnerabilities

1.2	*Strengthening of the capability to collect, process, and disseminate the information (cyber intelligence) and the capability to manage the resulting knowledge (knowledge management)*	a. Strengthen cyber intelligence capabilities b. Develop capabilities and procedures to monitor volumes of traffic and to correlate events with the goal of enhancing the capability to promptly detect anomalies associated with cyber threats and attacks c. Implement early warning procedures d. Develop integrated intelligence capabilities (across ministers and multi-sourced)
1.3	*Development of capabilities to contrast cyber threats*	a. Improve the capability to attribute a cyber attack b. *Cyber Situational Awareness* c. Facilitate agreements aimed at promoting info-sharing between the relevant public Administrations and the private sector, along the lines of already existing norms d. Strengthen the capability to respond to cyber incidents and to contrast cyber crime
1.4	*Development of key operational capabilities, in line with the Defense Directives in the cyber domain*	a. Implement the full operational capability of all structures devoted to the protection of the cyberspace, establishing the assets identified by the chain of command, and providing for their preparedness, training, leadership, protection, support and deployment b. Develop Command and Control structures that are able to plan and conduct military operations in cyberspace in an effective, prompt and distributed way (Operative Cyber Inter Forces Centre – "COCI")

1.5	*Development of digital forensics analysis capabilities*	a. Strengthen and disseminate the capability to acquire data through digital forensics techniques b. Increase "live digital forensics" capabilities c. Strengthen data analysis capabilities d. Develop "post mortem" digital analysis
1.6	*Lessons learned process*	a. Creation of a set of procedures and instruments aimed at recording, analyzing, appraising, and sharing the lessons learned in the management of cyber incidents

OPERATIONAL GUIDELINE 2

ENHANCEMENT OF THE ORGANIZATION, COORDINATION AND DIALOGUE BETWEEN NATIONAL PRIVATE AND PUBLIC STAKEHOLDERS

This guideline aims at enhancing the coordination and the cooperation not only between the various public sector stakeholders, but also between them and the private sector, which owns and operates critical national infrastructures. The full interoperability among all relevant stakeholders, including those at the international level, is the key to make this coordination and cooperation possible.

2.1 ***Integration***	a. Develop cooperation and trust between public and private sectors (including public utilities providers), also with a view to identify and mitigate vulnerabilities b. Facilitate the activities of formal working groups and communities of entities envisaging the participation of network operators and providers of ICT services, especially those focusing on identify standards, arrangements and procedures for supporting the functioning of the national CERT c. Strengthen info-sharing arrangements

2.2 *Infrastructures*	a. Formulate a methodology for the identification of ICT networks and computer systems that support critical functions b. Develop initiatives, solutions and tools for the management of cyber crises through a joint effort of all relevant authorities in charge of the protection of critical infrastructures, including ministries, the private sector, as well as other partner countries, with the aim to build a safe and resilient system c. Define specific evaluation standards and internal analysis communication formats for critical infrastructures and their potential vulnerabilities d. Prepare vulnerability mitigation strategies e. Set out minimum requirements for cyber defense, both in terms of instruments and procedures, for the protection of critical infrastructures
2.3 *Interoperability*	a. Ensure organizational interoperability and semantic coherence among all public Administrations, the private sector, the EU, and NATO, so as to allow for a common definition and understanding both of cyber events and of the protection and reaction procedures for dealing with cyber crisis

2.4	*Participation of private sector actors in bilateral and multilateral events concerning cyber security, also taking place at the international level*	a. Strengthen the specific channels devoted to the dialogue and consultation between the institutions and the private sector (whole-of-government approach) b. Arrange for joint missions in bilateral and multilateral contexts c. Enhance the private sector's participation in international exercises focusing on the protection of critical infrastructures relying on ICT networks and computer systems
2.5	*National coordination of the works done by the Council of the EU regarding the proposal of the Directive in matter of cyber security*	a. Define the national position with regard to Directive COM (2013) n. 48 final of the 7th February 2013, on the basis of the contributions provided by the interested Administrations

OPERATIONAL GUIDELINE 3

PROMOTION AND DISSEMINATION OF THE CULTURE OF SECURITY. TRAINING AND EDUCATION

Up until now, training and education activities in cybersecurity have addressed primarily specialized personnel operating or prospectively working in the cybersecurity sector. It is now of the utmost importance to promote and disseminate a Culture of Cybersecurity among the wider public, including citizens and personnel employed both in the public Administration and private companies.

3.1	***Development of concepts and doctrine***	a. Analyze the evolution of the National Strategic Framework, update the concepts and develop the doctrines related to cyber operations and activities, also through the identification of international best practices b. Improve at the national level, as well as at the NATO and EU level, the understanding of how dissuasion and deterrence may contain a potential escalation of a crisis in cyberspace
3.2	***Promotion and dissemination of the Culture of Cybersecurity***	a. Organize targeted initiatives for citizens, students, firms and public Administrations' personnel
3.3	***Education and training***	a. Participate in sensitizing activities coordinated by the European Union Network and Information Security Agency (ENISA) b. Raise awareness among decision makers on the effects and evolution of the cyber threat

c. Educate and train the personnel. Tailored training for personnel assigned to cyber operations and for those working in the public Administration who are in charge of the organization, management and protection of ITC networks and computer systems
d. Develop, verify and validate the operations carried out in cyberspace with the support of simulations, collective training and training-on-the-job
e. Merge all available training and education activities in the Ministry of Defence, and make them available to the personnel of other Administrations, of public and private sector firms, staff of the EU and NATO as well as nationals of partner countries
f. Organize, under the initiative of the Advanced School of Specialization in Telecommunications (SSST), specific courses, seminars, public lectures on subjects that are related to information assurance and ICT networks security and that pertain to the certification of ICT security compliance and to vulnerabilities analysis
g. Develop specific education programs in cooperation with the Advanced School for Magistrates and the schools for administrative and penitentiary personnel
h. Develop synergies with the academia with the aim to define ad hoc training courses for the personnel of public administrations and firms
i. Map the centers of excellence in the subject matter

OPERATIONAL GUIDELINE 4

INTERNATIONAL COOPERATION AND EXERCISES

The transnational nature and pervasiveness of the cyber threat require an international approach in which all like-minded States need to join forces in search for all possible synergies to collectively develop the capabilities required to cope with the threat. This, in turn, requires a common level of preparation and wide interoperability.

4.1	***Strengthening of bilateral and multilateral cooperation***	a. Create structured and cooperative relationships with the member states of the EU, NATO and other partner countries b. Ensure the highest possible level of integration and interoperability in the planning process and in the conduct of computer network operations through joint activities involving the Ministry of Defense, other Administrations, NATO, the EU as well as other countries c. Ensure the highest possible level of integration and interoperability of management processes of computer network operations – including norms and training activities – so as to share information and set up joint initiatives at bilateral and multilateral level, as well as with other relevant international forums (EU, NATO, OECD) d. Participate in multilateral organizations (EU, NATO, UN, OECD etc.) so as to have a comprehensive understanding and ensure a consistent national stance on the subject

		e. Support the full participation of the Italian judicial system in the European e-Justice Working Group so as to be able to develop the information-sharing platforms and provide the associated services, as they will be made available
4.2	*Exercises*	a. Organize, on a regular basis, national exercises in cybersecurity (i.e. Cyber Italy) b. Coordinate the national participation, both of public and private stakeholders, in exercises at the pan-European level (Cyber Europe), with the United States (Cyber Atlantic), and with NATO (Cyber Coalition)
4.3	*EU projects*	a. Promote and disseminate, also to the benefit of the private sector, information regarding initiatives and ways to be eligible for and participate in EU programs b. Optimize the access to EU funds c. Participate in projects financed by the EU, in particular in the so-called Advanced Cyber Defense Center (ACDC)

OPERATIONAL GUIDELINE 5

ATTAINING THE FULL OPERATIONAL CAPABILITY OF THE NATIONAL CERT, OF THE CERT-PA AND OF ALL MINISTERIAL CERTs

In order to set up prevention and reaction capabilities to a cyber crisis, it is necessary to develop Computer Emergency Response Teams (CERT) that provide technical assistance, research and development, education and information to their users and clients, whether public or private, and are able to operate both with a proactive and a reactive approach.

5.1	***Development of the CERT-PA and of the ministerial CERTs***	a. Integrate the structure of the CERT-SPC transforming it into CERT-PA, by identifying the necessary human resources and activating suitable head-hunting procedures, as well as adapting the technical and operational capabilities and the logistic infrastructures to ensure it is fully operative b. Establish a cooperation mechanism for the structures that deliver ICT security within public administrations, in particular the Local Security Units (ULS) and the Security Operations Center (SOC), promoting, where possible, their transformation into ministerial CERTs c. Foster the creation of Regional CERTs with the task of supporting local public administrations and implementing national rules and models of organization d. Adopt the procedures identified by the Agency for Digital Italy (AgID) e. Pursue a consistent level of security of the Data Centres and of the work environments of public administrations, as well as of the private firms managing national critical infrastructures

5.2	*Activation of the national CERT*	a. Identify the human resources and the operational capabilities for ensuring the activation of national CERT, initiating the procedure for personnel recruitment in the public Administration b. Stipulate agreements with public institutions and the private sector to implement cooperation and exchange of information through ad hoc auditions c. Start a trial phase and introduce essential services d. Adapt the technical and logistic infrastructures of the national CERT in order to guarantee it is fully operative
5.3	*Development of a national integrated Computer Incident Response Capability (CIRC)*	a. Seek collaboration and cooperation between ministerial CERTs and CERT-PA in order to be able to mitigate the effects of possible cyber events b. Support ministerial CERTs in the swift and effective recovery from computer incidents c. Develop a proactive and integrated approach in order to contain and mitigate threats to cyber security through the activation of an integrated database to gather incidents reports and archive the countermeasures undertaken; of an integrated system for alarm detection, online incident/intrusion detection, strong authentication, etc. d. Develop a proactive and integrated approach in order to contain and mitigate threats to cyber security through the activation of an integrated database to gather incidents reports and archive the countermeasures undertaken; of an integrated system for alarm detection, online incident/intrusion detection, strong authentication, etc.

e. Develop an integrated approach of reaction (resilience), following tested procedures for ensuring business continuity and disaster recovery
f. Develop incident response capabilities
g. Support the technical-functional and procedural evolution of capabilities that are similar to and in harmony with the NATO Computer Incident Response Capability – Technical Centre (NCIRC-TC) Technical Centre (CIRC-TC)

OPERATIONAL GUIDELINE 6

PROMOTION OF *AD HOC* LEGISLATION AND COMPLIANCE WITH INTERNATIONAL OBLIGATIONS

The fast pace of technological and computer advancements makes the norms regulating matters concerning ICT technologies rapidly obsolete. Therefore, these norms require regular revisions, update and integrations in order also to ensure a legal framework to the activities that are carried out with respect to cyber protection and ICT network security and to make users and administrators accountable for the actions they undertake in the domain under their responsibility.

6.1	***Revision and consolidation of the legislation in the field of ICT security***	a. Merge the current juridical knowledge gained in all public administrations in the field of cybersecurity b. Evaluate the alignment between the existing national legislation and the evolutions brought about by technological innovations, considering the possibility of carrying out legislative interventions that benefit from international best practices c. Finalize the normative framework defining standards and criteria to identify national public and private critical infrastructures supported by ICT networks and computer systems d. Update the legislation in the field of digital judiciary records

6.2	*Definition of a normative framework that is suitable to support activities concerning cybersecurity and, in particular, cyber operations*	a. Identify a national juridical framework that, in line with international norms, regulates – with a pre-emptive approach - all activities pertaining to cyber security, including computer network operations
6.3	*Attribution of responsibilities and sanctions in case of violations*	a. Define a legal framework and a reference methodology in order to identify the necessary technical instruments, including those pertaining to the routing of the attack, for the attribution of responsibilities (and of the related sanctions) in case administrators and users of networks of interest are responsible for security breach
6.4	*Proposals for the implementation of the Directive of the European Parliament and Commission concerning measures to ensure a high common level of network and information security across the Union*	a. Promotion of cooperation between public institutions and the private sector to bring forward proposals for the implementation of the European Directive concerning cybersecurity, with particular regards to the identification of technical and organizational measures aimed at increasing the level of security in the sectors identified by the same Directive

OPERATIONAL GUIDELINE 7

COMPLIANCE WITH SECURITY STANDARD AND PROTOCOLS

The compliance with national and international standards and security protocols makes it possible to guarantee a common and high level of cyber protection of computer systems and ITC networks.

7.1	*Standardization*	a. Update the national framework of reference of security standards and protocols in accordance with the norms ratified with NATO and the EU b. Adopt standards of reference for the authentication of, and authorization to the access to the networks of interest c. Produce binding guidelines for the adoption of the IPv6 Internet Protocol
7.2	*Documents of references*	a. Elaboration and publications of documents such as manuals, lists of standard procedures and recommendations (best practices of the field), uniform taxonomy and lexicon to be used for information exchange
7.3	*Review of the management and operational documents and manuals*	a. Review and update on a regular basis all documents (rules, procedures, etc.) concerning the management of critical infrastructures

7.4	*Security certifications and evaluation*	a. Manage the National ICT Security Certification Scheme for commercial ICT Products and Systems (dealing with non classified data) through the Computer Security Certification Organization (OCSI), that operates according to the international Common Criteria standard (ISO/IEC 15408) b. Keep up-to-date a national scheme for the certification of the processes used by computer systems, in compliance with standard UNI/ISO IEC 27001:2006 c. Ensure the "CE.VA" – Evaluation Center – is operative as a laboratory that evaluates the technical security of computer systems and ITC networks that deal with classified data d. Participate in the works carried out by the institutions that define the guidelines of mutual international recognition in the field of certification, in particular: the Common Criteria Recognition Arrangement (CCRA), that operates worldwide, and the Senior Official Group for Information Systems Security – Mutual Recognition Arrangement (SOGIS – MRA), that operates at the European level
7.5	*Verification of cyber defense measures applied to critical infrastructures*	a. Regular auditing of the systems of protection through technical and procedural tests b. Definition of an independent auditing system (for example external audit)
7.6	*Compliance*	a. Set up a system for the accreditation and auditing of the entities in charge of the emission of digital certificates of authentication

OPERATIONAL GUIDELINE 8

SUPPORT TO INDUSTRIAL AND TECHNOLOGICAL DEVELOPMENT

The complete reliability and security of hardware and software components manufactured in the EU or third countries, especially those that support critical infrastructures and other subjects with a strategic relevance for the country, can be reached only if all those involved in the value chain (hardware components producers, software developers, service providers of IT society) will make security a priority.

8.1 *Logistics*	a. Guarantee a supply chain of secure and resilient components, under the cybersecurity point of view, that is supported by flexible and fast validation, verification and certification processes b. Promote ICT innovation, through the promotion of vertical supply chain integration both at the national and EU level, in order to develop an industrial base that is competitive at the international level c. Strengthen bilateral and multilateral cooperation programs to promote national R&D activities in Europe and internationally
8.2 *Implementation of a governmental laboratory of comparative analysis*	a. Support the creation of a governmental laboratory of verification that conducts comparative analysis of ICT systems that are of interest to administrations and national critical infrastructures

OPERATIONAL GUIDELINE 9

STRATEGIC COMMUNICATION

The disclosure of the occurrence of a cyber attack and of the associated consequences is of strategic importance because the concerned administrations must be in the position to provide complete, correct, and transparent information about it, without creating unjustified alarm that could magnify the economic and social impact of the cyber attack.

9.1	***Strategic communication***	**a.** Develop a situational awareness of the content of information and alerts, in order to ensure an effective communication **b.** Establish a protocol for public communication aimed at giving a correct and transparent overview of voluntary and accidental cyber events as well as of the response and system recovery actions that are put in place

OPERATIONAL GUIDELINE 10

RESOURCES

In order to achieve an appropriate budget and resources allocation it is essential to conduct a cost analysis of occurred and potential cyber events, because the severity of the risk of a cyber event is proportional to the likelihood of its occurrence and the magnitude of its impact. Likewise, in order to prioritize the vulnerabilities it is essential to have the right elements for an economic assessment. A sound economic estimate could be of help in finding the right balance between the costs of and the need for investments both in the public and private sector.

10.1	***Financial planning and economic factors***	a. Define priorities and associated costs of cybersecurity and cyber defense measures for the protection of critical infrastructures and the development of key operational capabilities, both in terms of technical assets and capabilities and of human resources
10.2	***Measurement of the costs associated with cyber events***	a. Define standards to measure the direct and indirect costs associated with actual and potential cyber events (activities of detecting, remediation, bad reputation, loss of clients/ credibility/reliability/competitiveness, costs of service disruption, possible human loss, etc.) b. Analyze the correlations between critical/strategic infrastructures also in order to be able to quantify accurately the overall economic cost of a possible domino effect c. Develop a survey of the economic effects of cyber incidents and analyze potential scenarios

10.3	*Efficient spending*	**a.** Define norms and financial instruments to optimize and share expenditures related to cyber defense among Ministries, public and private sector, and possibly with other countries for the implementation of international cooperation programs
10.4	*Human resources*	**a.** Facilitate dialogue among ministries so to support integrated approaches to the recruitment of specialized personnel, also taking into account international best practices in this matter

OPERATIONAL GUIDELINE 11

IMPLEMENTATION OF A NATIONAL SYSTEM OF INFORMATION RISK MANAGEMENT

The protection of data from threats that could compromise their authenticity, integrity, confidentiality and availability is an essential component of this National Plan because information has a value by itself for any organization, whether public or private, and because it is the prime target of any cyber attack.

11.1 ***Methodology***	**a.** Identify at the strategic level a shared and unambiguous information risk management methodology, adopting a model for national ICT critical infrastructures in accordance with UNI EN ISO 27001:2011 **b.** Involve research centers and Universities so as to be able to adopt up-to-date risk management tools and procedures